Italy's DPA issues guidance whilst waiting for GDPR implementing Bill

The *Garante's* guidance deals with data portability, data protection officers and the lead supervisory authority. **Matteo Colombo** reports from Milan on other aspects of the guidance.

In Italy, the *Garante*, the Data Protection Authority, has for months been working to issue guidance on the new rules under the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"). But we are only at the beginning of a long march that will go beyond the fateful date of 25 May 2018.

Guidelines were published in July together with infographics and brochures which explain the new rules to the public and private sectors.[1]

The documents include recommendations on how to interpret the GDPR as well as recommendations for good practice. On consent of the data subject, the *Garante* specifies that, if collected before 25 May 2018, it remains valid if it fulfills all the requirements in Art. 6 GDPR (explicit consent for sensitive data and automated decision-making). Otherwise, it is advised to re-collect the consent of the parties concerned as required by the Regulation, if an organisation wants to continue to use consent as its legal basis.

Consent may not necessarily be "documented in writing" nor in "written form", even if this is a way to ensure that consent is unambiguous and freely given and "explicit" for special categories of personal data. Where processing is based on consent, controllers must be able to demonstrate that data subjects have consented to processing of their personal data (Article 7.1). With regard to information to be provided to data subjects, data controllers should verify compliance of current privacy notices. Internal organizational measures must be taken to ensure compliance with the timing of replying to Subject Access Requests. The deadline of one month for informing the data subject is clear, and it should be noted that Article 14, paragraph 3, states that information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month.

Response to a data subject must be written (can be in electronic form) by default, and the data controllers can allow data subjects to consult their personal data directly, remotely and securely.

Regarding the record of processing activities, the *Garante* specifies that it is not merely a formal fulfillment but an integral part of a proper personal data management system and accountability. For this reason, all data controllers and data processors are invited, irrespective of the size of the organization, to take the necessary steps to equip themselves with this record. They must carry out a thorough examination of the processing activities performed and their respective features, where not already done. The *Garante* is considering making available on its site a template for making a Record of Processing activities, which individual data controllers can integrate in appropriate ways.

> Unfortunately, activity on adapting Italy's national law to the GDPR has slowed down.

In case of a data breach, it is recommended that all data controllers always document the violations of personal data that have been suffered, even if not notified to the control authority and not communicated to the data subject, as well as the relevant circumstances, consequences, and measures adopted.

Timetable in Italy

Unfortunately, activity on adapting Italy's national law to the GDPR has slowed down and there is a risk that the rule will be postponed until after the general election scheduled for Spring 2018. But we very much hope that the legislator will understand the importance of having clear rules before the application of the GDPR.

The Law on European Delegation 2016-2017 (Law No. 163/2017) was published on 6 November 2017 in the Official Gazette of the Italian Republic. Article 13 of the Law delegates to the Government competence to adopt, within six months from the Law's entry into force on 21 November 2017, one or more legislative decrees which aim to adapt the national legal framework to the GDPR (Regulation (EU) 2016/679).

In particular, the Law states that the Government will be expected to expressly repeal the incompatible provisions of the Personal Data Protection Code, Legislative Decree No. 196/2003, and adapt the remaining ones to the GDPR.

Further, the Government is expected to empower the *Garante* to issue specific implementing decisions where appropriate, and review the criminal penalties provision and administrative penalties provisions for

AUTHOR

Matteo Colombo is Chief Executive, Labor Project, and President, ASSO DPO, Italy's association for data protection officers. Email: matteo.colombo@laborproject.it

REFERENCES

1 194.242.234.211/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf (in Italian)

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Australia's mandatory breach notification regime imminent

A notification duty will apply, from February 2018, to all private sector and not-for-profit organisations with an annual turnover of more than A$3 million. By **Elizabeth Coombs** and **Sean McLaughlan**.

From 22 February 2018, Australian Federal Government agencies and private businesses (including not-for-profit organisations) with an annual turnover of A$3 million or more, or that trade in personal information, will be required to comply with the Notifiable Data Breaches (NDB) scheme.[1] The protection of personal information is familiar territory internationally but not as familiar in Australia where the right to privacy is not recognised in the Constitution, not enshrined in a

Continued on p.3

Questioning 'adequacy'– Japan

An EU adequacy decision for Japan is expected in 2018. **Graham Greenleaf** analyses what the remaining challenges are.

Assessments by the European Commission of whether non-EU countries provide an "adequate" level of data protection so as to enable a positive EU decision[1] under Article 25 of the 1995 Data Protection Directive ("adequacy decisions") usually receive little discussion while the process is underway. It is often not until the near-final stage of decision-making, when the Article 29 Working Party (A29WP) of Data Protection Commissioners gives an Opinion on whether it supports a positive assessment by the Commission, that it even becomes public knowledge that an assessment is

Continued on p.6

Issue 150 **December 2017**

INTERNATIONAL report

ISSUE NO 150 DECEMBER 2017

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan.thomas@privacylaws.com

CONTRIBUTORS
Henry Chang
University of Hong Kong, Hong Kong

Elizabeth Coombs and Sean McLaughlan
Australia

Matteo Colombo
ASSO DPO, Italy

Scott Livingston
Simone IP Services, Hong Kong

Merrill Dresner
PL&B Correspondent

Patricia Gelabert
PL&B Correspondent

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Adequacy is a fluid concept

As we were going to print, the EU Article 29 DP Working Party published a working document on its adequacy referential. This document will be continuously reviewed and if necessary updated in the coming years, based on the practical experience gained through the application of the GDPR. The EU Commission is now actively negotiating with South Korea and Japan, the latter of which is expected to receive an adequacy determination in 2018 (p.1). Next it might be the United Kingdom's turn – a different situation altogether but perhaps not any easier, given the direction of travel in the UK.

Australia's mandatory data breach notification regime will be in force from February (p.1), and China has adopted a new Personal Information Standard (p.25). Other Asian developments include practical experience with mediation both in South Korea and Hong Kong. We have been very fortunate to speak to both countries' regulators when in Hong Kong (p.20 and p.22).

With regard to the EU GDPR, only Germany and Austria have so far adopted implementing laws. Italy's DPA has issued guidance whilst waiting for a GDPR implementing Bill (p.12), and Finland's working group is still considering several issues (p.13). In Spain, there is a data protection bill but many changes are expected (p.14).

Meanwhile the EU DPAs have threatened legal action to come next May unless the EU-US Privacy Shield is improved (p.17). The other 11 adequacy agreements are also being reviewed – the EU is asking for clarifications on their privacy safeguards. This assessment applies, for example, to Guernsey, which has just adopted a new law (p.21).

Something that throws the principle of defining a data controller back to the drawing board is blockchain. Read on p.18 about the other data protection issues which are related to Distributed Ledger Technology, of which the most prominent example is Bitcoin, the crypto currency.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK